



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/046,042	11/19/2001	Steven Siong Cheak Mok	1085-PWH	2086

60597 7590 09/20/2006

PATRICK W. HUGHEY
P.O. BOX 6553
PORTLAND, OR 97228

EXAMINER

HERRING, VIRGIL A

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 09/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/046,042	Applicant(s) MOK, STEVEN SIONG CHEAK	
	Examiner Virgil Herring	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10 July 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-4, 6, 7, 10-25 and 27-32 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-4, 6, 7, 10-25 and 27-32 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This action is responsive to the amendment filed 10 July 2006. Claim 26 is cancelled by this amendment, and claims 5, 8, and 9 were cancelled previously. Claims 1-4, 6-7, 10-25, and 27-32 are currently pending.

Response to Arguments

Applicant's arguments filed 10 July 2006 have been fully considered but they are not persuasive.

Regarding claim 1, applicant argued that Belcher et al (US Patent #6,393,045) does not teach a transponder writer. Applicant's position is that the transponders of Belcher are one-time-use devices that there "is no need to have the object ID information replaced." Examiner agrees that there is no need to replace the object ID information, but notes that this is not what claim 1 says. Claim 1 merely requires a transponder writer operable to send an object ID to the transponder, which the transponder then stores in its memory, which Belcher does include. Applicant's assertion that "on-the-fly" and "at the time of use" does not refer to re-use of the transponder is unfounded based on the disclosure of Belcher. The sentence in question actually states "For on-the-fly applications, such as in the transportation industry, the transponder's memory may be programmed magnetically by means of a write coil of a magnetic field generator, into which the transponder-embedded Mylar strip is inserted at the time of its use." Nowhere does this sentence indicate that the transponder is for a

single use only. In fact, the opposite is implied, because figure 4 shows “a microcircuit implementation of the tag-embedded transponder of FIG. 3”, in which the memory 110 is clearly stated to be an EEPROM.

With regards to claim 1, applicant also argued that the system of Carroll et al (US Patent #4,952,928) does not require the ID information stored in the transponder to be replaced because of the intended use of the invention of Carroll. This argument is not applicable to the patentability of claim 1 over Carroll, because the intended use has no bearing on the structure or functionality of the invention. Applicant further argued that both Belcher and Carroll merely identify the object being tracked by the tag, without indicating the security status of the wearer. The examiner has found no such indication of security status in the limitations of claim 1, and thus this argument is irrelevant. However, the examiner also points out that the security status of a person fitted with the transponder of Carroll would be implied, because the transponder is only used to track individuals who are currently under house arrest (and therefore, presumably, are currently being tried for or have been convicted of a crime).

Regarding claim 11, applicant argued that the transponder reader of Carroll is not “portable” given the broadest reasonable interpretation. Examiner notes that the broadest reasonable interpretation of “portable”, as found in the American Heritage College dictionary, is “carried or moved with ease”. Examiner notes figure 5 of Carroll, a depiction of the transponder reader, and the description of the figure found at column

Art Unit: 2132

13, lines 43-62. 100 and 102 of the figure are stated to be telephone jacks, which mean that the transponder reader is approximately 2"x3"x1", not including the cord and plug assembly. Certainly a device of 6 cubic inches conforms to the broadest reasonable interpretation of portable. Applicant further argued that Carroll teaches away from a portable transponder reader. Examiner disagrees, for the reasons stated above.

Regarding claim 13, applicant argued that Carroll does not include an access database storing access parameters related to the secured area and transponder carrier. Examiner respectfully disagrees, noting column 3, lines 48-68 as evidence. Carroll clearly indicates the use of a plurality of transponders and readers to track multiple people over a large (i.e. city-scale) area. Column 4, lines 18-53 expand on this by stating that the system can be used to verify that the person wearing a specific transponder complies with defined restrictions, such as visiting a specific location (presumably a parole officer or equivalent supervisor) at certain times (lines 48-53). Clearly advanced functionality of this type would require a database to define the rules.

Regarding claim 14, applicant states that, as a house-arrest monitoring system, Carroll would not include notifications of a transponder in an unauthorized area, because the transponder must always be at the individual's house. As described above, the system of Carroll clearly does not limit the individual to one location, but rather, tracks a plurality of transponders over a large area. Because the system includes directives for where a transponder is supposed to be at a given time (Col. 4,

Art Unit: 2132

lines 48-53), the inverse would be that the system includes directives for where the transponder is NOT supposed to be at a given time.

Regarding claims 19 and 20, applicant argued that Carroll and Belcher do not make reference to a replacement identifier, nor do they require one. Examiner disagrees, for the reasons stated above.

Regarding claims 24 and 30, applicant states that the claims are allowable for the same reasons as the previously argued claims. Examiner disagrees for the reasons discussed previously.

Regarding claim 25, applicant has amended the claim to include the limitation of cancelled claim 26 that the transponder reader is portable, and argues that this distinguishes the claim over Carroll and Belcher. Examiner disagrees, for the reasons cited above in reference to claim 11.

Regarding claim 32, applicant argued that Chien (US Patent #6,512,478) does not teach a transponder reader including a motion detector. Examiner respectfully disagrees, noting column 1, lines 16-28 as evidence, which state both motion detectors and RF tags in location/position systems to be a part of the prior art.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim 25 is rejected under 35 U.S.C. 102(b) as being anticipated by Carroll et al (US Patent #4,952,928).

With regards to claim 25, Carroll et al disclose an RF transponder reader operable to send an interrogation signal to an RF transponder having a unique identifier and receive from the transponder, in response to the interrogation signal, the unique identifier, the reader being a portable unit (Col. 2, Lines 25-31) and operable to transmit the unique identifier to a security processor for identity verification; (Col. 2, Lines 20-30) wherein the location of the transponder is determined from the location of the transponder reader. (Col. 2, Lines 41-47)

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-4, 6-7, 10-25, 27-29, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carroll et al (US Patent #4,952,928) in view of Belcher et al (US Patent #6,393,045).

With regards to claim 1, Carroll et al (US Patent #4,952,928) disclose a security system for facilitating transponder carrier identification and tracking within a secure area comprising:

an RF transponder having a memory in which is stored a unique identifier;
(Col. 2, Lines 20-23)

the transponder including a transmitter to transmit the unique identifier;
(Col. 2, Lines 20-23)

a transponder reader to receive from the transponder at least the unique identifier of the transponder; (Col. 2, Lines 25-30)

such that the transponder reader interrogates the transponder and, in response to the interrogation, receives from the transponder at least the unique identifier of the transponder; (Col. 2, Lines 20-23)

wherein the location of the transponder is determined from the location of the transponder reader. (Col. 2, Lines 41-47)

However, Carroll et al do not expressly disclose a security system for facilitating transponder carrier identification and tracking within a secure area comprising:

a transponder writer operable to send a replacement unique identifier to the transponder, the transponder replacing the identifier in the transponder memory with the replacement identifier;

However, Belcher et al (US Patent #6,393,045) teach a way to differentiate between operations that read from or write to memory contained within a transponder tag (Col. 6, Lines 32-38). Belcher et al and Carroll et al are analogous art because both involve interrogating a transponder and receiving, in response, a unique identifier which indicates the subject to which the transponder is affixed. In light of the teachings of Belcher et al, it would have been obvious to one skilled in the art to use a transponder with a writable memory in the identification and tracking system disclosed by Carroll et al. The motivation for doing so would have been "for on-the-fly applications" (Belcher et al, Col. 9, Lines 55-59). The examiner notes that, although the Belcher et al teach the use of magnetic field links rather than radio communications, the system is still used to write data to a memory device contained within an electronic transponder.

The examiner notes that claim 1 incorporates all the limitations of claims 24 and 30. Thus, claims 24 and 30 are rejected on the same grounds as claim 1.

With regards to claim 2, the combination of Carroll et al and Belcher et al as described above includes (from Carroll) a security system according to claim 1, wherein the transponder has a fixed unit identifier serving to identify the transponder, the fixed unit identifier being a separate identifier to the unique identifier. (Col. 4, Lines 56-60 discuss an encoded signal that identifies the person being monitored; Col. 7, Lines 59-64 discuss a code that identifies the tag itself)

With regards to claim 3, the combination of Carroll et al and Belcher et al as described above includes (from Carroll) a security system according to claim 2, wherein the unique identifier comprises an identity code. (Col. 7, Lines 59-64)

With regards to claim 4, the combination of Carroll et al and Belcher et al as described above includes a security system according to claim 1, wherein the unique identifier is encrypted and assigned by a security processor. (This feature is inherent to the combination. The system of Carroll is used for tracking prisoners, so the assignment of transponder codes would be done by security personnel from the prison, using a transponder writer.)

With regards to claim 6, the combination of Carroll et al and Belcher et al as described above includes (from Carroll) a security system according to claim 1, wherein the transmitter is a contactless transmitter operable to transmit RF signals. (Col. 1, Lines 53-57)

With regards to claim 7, the combination of Carroll et al and Belcher et al as described above includes (from Carroll) a security system according to claim 1, wherein the transmitter is a contact transmitter operable to send signals to a unit in contact with the transponder. (Col. 10, Lines 34-36)

With regards to claim 10, the combination of Carroll et al and Belcher et al as described above includes (from Carroll) a security system according to claim 1, wherein the transponder reader is mounted within the secure area and has a location code which provides information as to the location of the transponder reader. (Col. 2, Lines 42-48; a large monitored area with a plurality of field monitoring devices would inherently include information about where the FMD is located)

With regards to claim 11, the combination of Carroll et al and Belcher et al as described above includes (from Carroll) a security system according to claim 10, wherein the transponder reader is portable and operable within the secure area. (Col 2, Lines 26-31; if the FMD is to be placed "at the location where the individual is to be confined," it must be portable in order to get there)

With regards to claim 12, the combination of Carroll et al and Belcher et al as described above includes (from Carroll) a security system according to claim 1, wherein the transponder reader has a predetermined interrogation range such that a transponder within the interrogation range will receive an interrogation signal from the reader and will respond thereto by sending its unique identifier, and so determine the location of the transponder. (Col. 2, Lines 20-23)

With regards to claim 13, the combination of Carroll et al and Belcher et al as described above includes (from Carroll) a security system according to claim 1, further

Art Unit: 2132

comprising a security processor having an access database setting out access parameters for the secure area and a carrier of a transponder, the security processor being operable to receive information from the transponder reader comprising at least the unique identifier of an interrogated transponder and the location of the transponder reader. (Col. 2, Lines 41-47; As disclosed, the "central computer" stores information relating when a transponder is supposed to be near a specific FMD out of a large number of possible FMDs.)

With regards to claim 14, the combination of Carroll et al and Belcher et al as described above includes (from Carroll) a security system according of claim 13, wherein the security processor determines from consultation of the access database whether the carrier is authorized to be in the vicinity of the interrogating transponder reader and further determines what, if an, action needs to be taken. (Col. 2, Lines 47-52; Because the system is used for tracking parolees or those under house arrest, it is inherent that violations of the predetermined guidelines as to where the person is allowed to be would result in notification of the authorities.)

With regards to claim 15, the combination of Carroll et al and Belcher et al as described above includes (from Carroll) a security system according to claim 13, further comprising an actuator controllable by the security processor to affect operation of a device in response to a condition determined by the security processor. (Col. 10, Lines 36-38)

With regards to claim 16, the combination of Carroll et al and Belcher et al as described above includes (from Carroll) a security system according to claim 15, wherein the device activated by the actuator is selected from the group consisting of: an image capture device; an alarm; an alert system; a lock; an emergency door release; a speaker; and a communication device. (Col. 1, Lines 25-29; Because the disclosure of column 1 discusses the use of transponder tracking for the purpose of "confining [an] individual to a designated area," attempts to leave that area would inherently result in the activation of an alarm, an alert system, a lock (specifically, unlocking a door so security personnel can enter the area), a speaker (specifically, the speaker on a portable radio carried by security personnel), and a communication device (the aforementioned portable radio). (Col. 10, Lines 36-38 specifically mentions a video capture device)

With regards to claim 17, the combination of Carroll et al and Belcher et al as described above includes (from Carroll) a security system according to claim 1, wherein the transponder is configured as a card having a contact terminal. (Col. 10, Lines 34-36)

With regards to claim 18, the combination of Carroll et al and Belcher et al as described above includes a security system according to claim 17, wherein a card reader/writer is provided having a contact region compatible with the card contact terminal, wherein the transponder is addressable by the card reader when the terminal and contact region are in contact with one another. (Carroll et al Col. 10, Lines 34-36,

Art Unit: 2132

wherein the "holding receptacle" that reads the transponder is modified to include writing to the transponder as taught by Belcher et al.)

With regards to claim 19, the combination of Carroll et al and Belcher et al as described above includes (from Belcher) a security system according to claim 18, wherein the card reader/writer is operable to write the replacement unique identifier to the transponder. (Col. 6, Lines 32-38)

With regards to claim 20, the combination of Carroll et al and Belcher et al as described above includes a security system according to claim 18, wherein the card reader/writer is integrated with an identification authentication device so as to authenticate the identity of a carrier of the transponder prior to writing a replacement unique identifier to the transponder of the carrier. (Carroll et al, Col. 10, Lines 35-47, wherein the transponder reader is a reader/writer as taught by Belcher et al)

With regards to claim 21, the combination of Carroll et al and Belcher et al as described above includes a security system according to claim 1, wherein the carrier is selected from the group consisting of: personnel (Carroll et al, Col. 1, Lines 23-25); a vehicle (Belcher et al, Col. 1, Line 31, wherein the shipping container implies the presence of a vehicle); and a hardware product (Belcher et al, Col. 1, Lines 30-31).

Art Unit: 2132

With regards to claim 22, the combination of Carroll et al and Belcher et al as described above includes a security system according to claim 1, wherein the unique identifier has an expiry time after which the unique identifier is no longer valid. (The combination as currently described includes a reader/writer that the carrier must be nearby either constantly or at a certain time. In the case of the check-in time, the unique identifier would expire at that time, while the carrier is close enough to the writer to receive a new unique identifier.)

With regards to claim 23, the combination of Carroll et al and Belcher et al as described above includes a security system according to claim 1, wherein communication between at least some of the components of the system is enabled by one or more of the Internet, wireless connection, hardwire connection, and intranet. (The combination as described uses wireless transponders. At column 2, lines 36-40 of Carroll et al, the field monitoring device uses a hard-wired telephone connection to transmit information over the Internet to a central computer. Column 9, lines 16-25 of Carroll et al also discloses other computers connected to the central computer to form a local network with the central computer, in other words, an intranet).

With regards to claim 29, the combination of Carroll et al and Belcher et al as described above includes (from Carroll) an RF transponder reader according to claim 25, wherein the reader incorporates a cellular telephone system. (Col. 19, Lines 51-54)

With regards to claim 31, the combination of Carroll et al and Belcher et al as described above includes (from Carroll) a security system according to claim 20 wherein the identity authentication device includes any one or a combination of: a keypad to receive an alphanumeric code or biometric authenticator, such as a finger print or retinal scanner. (Col. 10, Lines 61-64; The examiner notes that alphanumeric passwords were used in security long before biometrics, and thus would also have been envisioned by Carroll et al for the identification of a carrier of a transponder.)

Claims 27, 28, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carroll et al (US Patent #4,952,928) in view of Belcher et al (US Patent #6,393,045) and further in view of Chien (US Patent #6,512,478).

With regards to claim 27, the combination of Carroll et al and Belcher et al as described above does not include an RF transponder reader according to claim 25, wherein the reader is integrated with a data archiving system.

However, Chien teaches a position location system for tracking an RF transponder tag wherein a base station for interrogating the tags can be embodied as a laptop computer or PDA (Col. 7, Lines 30-33). The examiner notes that laptop computers and PDAs are both electronic systems for archiving data, either in a hard drive or in memory. At the time of the invention, it would have been obvious to one skilled in the art to apply the teachings of Chien to the combination of Carroll et al and

Art Unit: 2132

Belcher et al, the field monitoring device of Carroll et al would be embodied as a data archiving device, such as a laptop computer or PDA, as taught by Chien. The motivation for this combination would have been to provide a monitoring device that could take advantage of Internet-ready wireless devices. (Chien, Col. 15, Lines 23-25)

With regards to claim 28, the combination of Carroll et al and Belcher et al, further modified by the teachings of Chien as described above would include (from Chien) an RF transponder reader according to claim 27, wherein the data archiving system is a personal digital assistant. (Col. 7, Lines 30-33)

With regards to claim 32, the combination of Carroll et al and Belcher et al as described above does not include a security system according to claim 1 wherein the transponder reader further includes a motion detector, such that on detection of movement within a detection zone, the transponder reader sends an interrogation signal to determine an identity of a user causing the movement.

However, Chien teaches a position location system for tracking an RF transponder wherein the transponder tag can conserve power by limiting its transmissions to times when it detects itself moving (Col. 1, Lines 16-28; Col. 25, Lines 42-44). Carroll et al disclose that transponders can be either active (internal power supply and constant transmission) or passive (inductive power supply, and only transmits when near a reader). Clearly, a passive transponder would not employ a

Art Unit: 2132

motion detection system in the transponder itself. However, at the time of the invention it would have been obvious to one skilled in the art to apply the teachings of Chien in a transponder tracking system such as the one disclosed by Carroll et al by using motion detectors in the tags themselves for active transponders, and using motion detectors in the field monitoring devices for passive transponders. The motivation for doing so would have been to conserve power by only communicating during periods of activity (Col. 1, Lines 16-28; Col. 25, Lines 42-44).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Virgil Herring whose telephone number is (571) 272-8189. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Virgil Herring *VH*
Examiner
Art Unit 2132

VH

Gilberto Barron Jr.
GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100